IAB Minutes

February 15, 2006

The Interagency Advisory Board (IAB) meeting convened on Wednesday, February 15, 2005 at 9:00 AM at the George Washington University (GWU) Marvin Center in the Grand Ballroom. The meeting was chaired by Mike Butler. After his introductory remarks, a series of presentations were given regarding the First Responder Partnership in National Capital Region (NCR).

A. First Responder Partnership Initiative – Ken Wall (DHS). The overview of the National Capitol Region partnership was discussed:

- Focus is Trust & Verification of Identity and Role Across Multi-Jurisdictions
- Objective – incident management: get right people with right skills to right place at right time
- Strategic Objectives
    1. Establishment of a multi-jurisdictional identity trust model
    2. Categorize all emergency response or critical infrastructure support personnel
    3. Integrate identity and NRP/NIPP category information into existing authoritative human resources databases/directories
    4. Standardize NRP/NIPP occupation sub-categories and qualifications
    5. Conduct exercises to integrate use with response requirements and applications development
- The goal is to establish *multi-jurisdictional identity interoperability*
- The partnership is establishing common processes for applicant, sponsor, enrollment official, registrar, issuance official, and validation & revocation authority

B. First Responder: Region 3 - Gordon Woodrow (DHHS). Key Points:

- Identity is key to achieving goals
- Working with partners in Region 3 state and local governments

C. First Responder: Federal - Lemar Jones (Pentagon Force Protection Agency). Key Points:

- Problem on 9/11 – key personnel couldn't cross lines to get beck to Pentagon
- Winter Fox – 2/23/06 - exercise to demonstrate interagency interoperability
- Hosted by Pentagon
- Proof of Concept of the *First Responder Authentication Card*
- IAB members are invited as spectators. Call 703-614-8634 to register

D. First Responder: DC - Robert LaGrande (DC-Office of CTO). Key Points:

- A critical component is basic communications for first responders
- Previously this was a patchwork of stovepipes that did not interoperate
- Moving to a comprehensive NCR Data Interoperability Communications Architecture:
    1. Fiber Optics backbone for voice, data, video
    2. Wireless broadband for seamless interoperability

3. Have completed Requirement's and Design Phase
4. Will include data Exchange Hubs to manage large volumes of data

- Goal is standardized incident management across jurisdictions that will enable machine-read information to determine access privileges for granting access into, out of, and within various areas as required
- 3 phase implementation: Limited (thru 2/28), Regional (7/30), Complete (9/30/08)

E. Virginia FRAC - Mike McAllister and Duane Stafford (VDOT). Key Points:

- Issuing First Responder Access Card (FRAC) to federal, state & local government
- Working with DHS to incorporate FIPS 201
- Led by VDOT Security and Emergency Management Division (SEMD) Transportation Protective Security Section (TPS)
- Used for Identification, Physical Access, Incident Response Site Access
- Developed FRAC policy, embracing HSPD-12 and FIPS 201
- Developed FRAC Request Form with DHS, may convert to electronic form
- FRAC Open Issues:
    - Digital photo must be accessible prior to PIN input.
    - Availability of Approved Products List Vendor and Accreditation (GSA).
    - NACI requirement solution for State governments.
    - Cardholder Naming convention must be clarified.
    - Color-Coding for Employee Affiliation must be clarified.

F. Maryland FRAC - Brad Jewitt (MDOT). Key Points:

- Have begun issuing Maryland FRAC
- Part of Port of Baltimore ACS Upgrade
- Performed in partnership with Baltimore Metro First Responders
- Alpha Testing Phase: 2000 FRAC Seats (Mobile Solution)
    - To be part of Winter Fox Demonstration 2/23/2006
    - Concept of Operations / Business Rules
- Beta Testing phase to include Brick and Mortar Site
- FRAC Penetration includes:
    - MD National Guard
    - Coast Guard
    - 8 of 23 Counties and Baltimore City (NCR / Baltimore)
- Future plans include strategic implementation plan for State across all ESFs

G. First Responder: Private – John N. Petrie (George Washington University). Key Points:

- Credentialing program is most important move forward by DHS since 9/11
- 15% of DC are faculty, staff, or students
- Entities such as GW (20,000+ pop., 125+ facilities) may strain public sector.
- Critical services and access to sensitive facilities must be continuously provided.
- Credential critical staff meets these needs, gives private sector responders/incident

teams creditability via universally recognized credentials.
- Self sufficiency will allow first responder resources to be utilized elsewhere.
- Eases access for thousands of employees commuting from MD, VA, WV, and PA who are separated by layers of local, state, and federal law enforcement agencies each with control points or perimeters.

H. Handheld RFI Update–Frank Jones (DoD). Key Points:
- RFI was released in December
- Vendor response has been stellar
- Team is creating a report to be ready by 3/21
- Unsure of how widely the report can/will be distributed as many responses included proprietary information
- Looking for volunteers to support, want team to be 75% non-Dodd

I. FIPS-201 Evaluation Program Progress – Judy Spencer (GSA). Key Points:
- Card Reader Interoperability Task:
  - About 66% complete
  - FIPS 201 Category List has been revised, 19 remaining categories have been mapped to Requirements Traceability Matrix
  - Reader categories are being revised to reflect use case
  - Test fixture prototype is being developed
  - Card/reader requirements document is nearing completion
  - Next major milestone is to validate card/reader requirements
- FIPS 201 Evaluation Lab Development Task:
  - About 20% complete
  - CONOPS, Configuration Management Plan, and Approval Procedures Template are all completed
  - Next major milestone is to review web-enabled information source
- Evaluation Program Technical Working Group (EPTWG)
  - Desire more technical input from reader & card manufacturers.
  - Looking for engineers who can meet in person, weekly, March thru April to review, comment on, and revise reader & card test procedures
  - Contact April Giles at april.giles@gsa.gov or 1.202.501.1123 to help
- RFI Status Update
  - Received 71 unique responses, 13 indicated “turn key” service capability
  - Cost data generally consistent, some questions regarding what is included
  - Conclusion – Industry is prepared to provide the services required by FIPS-201 for Enrollment and Card Management
  - Next Steps include developing a high level architectural concept and preparing technical specifications for a managed solution
  - Awaiting results from two agency data calls – due Feb 24, 2006.

J. Dire Warning – Ron Martin (DOC). Key Point:

- 254 days left until we cross over to "Phase Two"

K. Physical Access Synergy – Tony Cieri (IAB). Key Points:

- Objectives are to ensure that:
  - No conflict or ambiguity in FIPS-201 or related documentation as they apply to PACS
  - Industry Standards are developed by SIA that are in synergy to Federal Requirements
- Working to ensure PAIIWG, SCA, an SIA are all in sync

L. Status Training Modules – Andrew Goldsmith (DOI). Key Points:

- Continuing development of a series of web-based training modules and tools
- For management, administrators and users
- Modules delivered 10/03/2005:
  1: PIV Overview www.usalearning.gov/coursecatalog/index.cfm?fuseaction=oltovervie
  2: PIV Roles and Responsibilities www.vodium.com/goto/blm/hspd12.asp
- Modules scheduled for Spring 2006 delivery:
  3: Privacy Awareness
  4: Administrator (technical explanation)
  5: Appropriate Uses
- Working with USALearning to host all five modules
- Two versions of each module likely:
  - Base version that runs on every platform
  - Content-rich version with multimedia for those platforms that support it

M. Backend Authentication Schema Working Group – Jonathan Baldwin (DOD). Key Points:

- Government only membership met several times over the last month
- Expanding to include other interested parties (Industry or government):
- Next meeting: conference call, Tuesday, 28 February, 2-4pm EST
- Contact jonathan.baldwin.ctr@osd.pentagon.mil if interested

N. Document Revision Progress – Curt Barker (NIST). Key Points:

- Focus is on stability as we try to improve
- We can't do anything that would invalidate cards that are just now reaching the final stages of validation.
- FIPS 201-1
  - Accommodates of OMB Memorandum M-05-24
  - Provides for interim issuance based on National Criminal History Check
  - Requires electronic indication of interim issuance on the PIV card
  - Signed by the NIST Director
  - Awaiting signature of the Secretary of Commerce.
- SP 800-73

- Adjustments to accommodate SP 800-76
- Changes to biometric storage formats
- Incorporates previously posted errata
- Eliminates requirement to provide user PIN before permitting access to public PKI certificate information
- Proposes changes posted for public comment (due before March 2006)

- SP 800-85A
  - Separates conformance testing of card commands and data model
  - To be posted February 16 at csrc.nist.gov/piv-program
  - SP 800-76 data model conformance requirements to be in SP 800-85B
- Subsequent Revisions
  - Staffing Federal Register Notice requesting change recommendations
  - Anticipate posting shortly
  - Plan workshops to discuss a) need for change, b) impact on standards stability, and c) priority and schedule determination

O. Cryptographic Migration Plan – Tim Polk (NIST). Key Points:

- FIPS 201 addresses cryptography via SP 800-78 and the FPKI *Common Policy*
- The Common Policy and SP 800-78 state migration timelines differently.
- Consistency is being pursued by NIST
- Changes to the FPK Common Policy have been in progress for 2½ months, and were final as of 5 PM Monday
- Timeline for cryptographic migration is as pragmatic as possible, but …
- Migration options are constrained by Moore's Law, which is not negotiable!
  - 80 bit cryptography (1024 bit RSA and 160 bit ECC) is *mostly* dead.
  - Authentication keys: 80-bit strength is fine through 2010
  - Signatures, confidentiality keys: need to replace 80-bit crypto *before* 2010
- RSA 1024 is widely used, so it is permitted under SP 800-78 and Common Policy
- ECC 160 not yet widely used
- 99% of applications in place today will work with 2048-bit cryptography
- Do not believe the impact on the application space is a problem
- Rather, the problem/tricky space is to move from SHA-1 to SHA-224.

P. Closing Comments – Mike Butler (DoD). Key Points:

- Now is the time for departments and agencies to step up and help fashion the outcome of the various working groups
- No one wants this to be a solely DOD activity
- Send people - technical people - to support these work groups

The IAB Meeting was adjourned at 11:34 AM.